UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

RYAN BERRIS,

Plaintiff,

v.

SUNG-FUNG CHOI, *et al.*

Defendants.

Case No.: 1:23-cv-04305 (AS)

ESI PROTOCOL

The parties have agreed to and hereby stipulate to the following provisions concerning production of electronically stored information:

I. Definitions

A. "Electronically Stored Information" or "ESI", as used herein, means and refers to digital or computer generated information or data of any kind, stored in or located on computers, file servers, cloud-based servers, discs, back-up tapes, phones, chat systems, messaging applications (including, but not limited to, SMS, iMessage, WhatsApp, Signal, WeChat, Telegram, Instagram, etc.), or other virtualized devices or media.

II. Collection, Preservation and Search Terms

A. The parties will reasonably cooperate to disclosure and identify the ESI systems that may contain relevant and/or responsive ESI.

B. The parties agree to disclose and, if appropriate, meet and confer regarding, custodians that may have in their possession, custody or control relevant and/or responsive ESI.

C. Nothing in this protocol shall be construed to affect the admissibility of discoverable ESI. All objections to discoverability or admissibility are preserved.

D. The parties agree to disclose search terms and, if appropriate, meet and confer regarding the use of reasonable search terms including searching using file types, email domains and date ranges for relevant custodians.

III. Filtering

A. De-Duplication: a party is only required to produce a single copy of responsive information. De-duplication shall be done based upon a commercially accepted method (e.g. MD5 hash values). Duplicate materials will be identified at the family level. Email attachments, however, will only be de-duplicated if the parent email is also a duplicate. Moreover, loose electronic documents will not be de-duplicated against email attachments.

B. De-NISTing: Electronic file collections will be De-NISTed, removing commercially available operating system and application file information contained on the current NIST file list

IV. Production Format of Paper or Scanned Records

A. The parties will produce paper records scanned or otherwise converted into electronic form or documents otherwise maintained in static image format in the following format if reasonably feasible:

B. Where possible, all documents shall be scanned to 300 DPI Group IV Black & White Tagged Image File Format (.TIFF or .TIF) files. TIFF files shall be produced in single-page format and 81/2 x 11 inch page size (except for documents requiring a different page size). Each image file should have a unique file name which shall be the Bates number of the page.

C. In scanning paper documents, distinct documents should not be merged into a single record, and single documents should not be split into multiple records (i.e., paper documents should be logically unitized). The parties will make reasonable efforts to have their vendors unitize documents correctly and will commit to reasonably address situations where there are improperly unitized documents.

D. Color documents (e.g., color photographs or graphical representations in color) shall be scanned as black & white, single-page TIFF images in accordance with the technical specifications set out above. A party shall produce color copies of specific documents pursuant to reasonable and proportionate requests made by another party where color is necessary to interpretation of the document. If color images are required, the files shall be delivered in single page, JPEG format.

V. Production of ESI

A. The parties will produce ESI in 300 DPI Group IV Black & White Tagged Image File Format (.TIFF or .TIF) files. TIFF files shall be produced in single-page format and 81/2 x 11 inch page size (except for documents requiring a different page size) along with corresponding image load files (e.g., .OPT, LEP, DII file). All TIFF files are to be provided with an accompanying searchable text (.TXT) file, and such text files shall contain the full text extraction. Extracted text will not be provided for electronic documents that have been redacted (e.g., for privilege, protected personally information or non-relevant trade secrets) because the extracted text would reveal the redacted information. Instead, these files should be run through an OCR process to capture the visible text only and the results exchanged in lieu of the original extracted text.

B. Word documents will be produced in the above format with tracked changes and comments showing.

C. Presentation files, including but not limited to Microsoft PowerPoint files shall be processed in the above format with images displaying comments, hidden slides, speakers' notes and similar data. Presentation files shall be provided in both image and native format.

D. During the process of converting ESI from the electronic format of that application in which the ESI is normally created, viewed, and/or modified to TIFF, metadata values should be extracted and produced in a load file ("metadata load file").

E. The metadata values that are to be extracted and produced in the metadata load files – where reasonably available and where permitted under applicable international privacy regimes (.DAT file using concordance standard delimiters) should conform to the fields set out in **Appendix 1**.

F. Messages extracted from mobile messaging applications should, in addition to including the body text of any message, be produced in such a manner as to permit identification of: (1) the messaging application associated with message; (2) the sender of a message (i.e., by username, phone number, or other identifier); (3) participants (as identified by username, phone number, or other identifier) in a messaging group, including when each participant was added to or left such group, as well as the designated name, if any, of such messaging group; (4) the order in which messages were sent and received; (5) calls made within the messaging application; (6) all attachments or photos transmitted within the messaging application; (7) the date and time (including time zone information) at which the message was sent, received, and read; and (8) whether a message or messaging group was deleted.

G. All date fields will be formatted MM/DD/YYYY and all time fields will be formatted HH:MM:SS where reasonably feasible.

H. Any party may add to its production one or more metadata fields in addition to those enumerated above and in Appendix 1, such additions may not be used to obligate any other party to provide additional fields of any type.

I. Notwithstanding any provision of this protocol, a party may request specific metadata in conjunction with a specific document request or through specific instruction to requests for production if relevant and proportional to the needs of the case. To the extent that the responding party objects to such request for metadata, they shall be required to state the specific nature of such objection without reliance on this Protocol. If the parties are unable to resolve any such objection by meeting and conferring, the requesting party may seek relief from the Court, which may order the production of such requested metadata without limitation to the required fields enumerated in this Protocol. A party shall not be obligated to re-collect documents based on requests pursuant to this provision.

J. To the extent reasonably available, the "Custodian," or "Source" field with respect to ESI gathered from an individual's hard drive will provide metadata sufficient to identify the individual custodian from whose hard drive such ESI has been gathered.

K. A party may de-duplicate ESI globally or across more than one custodian provided that the producing party identifies all custodians within the production from which each such file or document was collected and deduped from the collection during processing.

L. A party shall produce native versions of specific documents in response to relevant and proportionate requests from another party where a native version of the document is necessary to the interpretation of the document.

VI. Production of Excel and Database ESI

A. Unless such materials contain privileged information, MS-Excel spreadsheets and similar type databases (e.g., MS Access) shall be produced in native format with a TIFF placeholder. The metadata load file shall contain a link to the produced MS-Excel spreadsheets and databases via data values called "Native Link." The Native Link values should contain the full directory path and file name of the MS-Excel spreadsheet or database as contained in the produced media. The Native Link field should be included in the .dat file specified above. The obligation to produce TIFF versions shall not apply where the TIFF version cannot be rendered in a readable or legible manner.

B. Production of responsive data contained in relational databases other than MS-Access should be achieved via report or export of such data to MS-Excel spreadsheets or .csv files that will be produced, if reasonably feasible. If this is not reasonably feasible, the parties will meet and confer regarding a reasonable format.

C. To the extent such material contains information subject to a claim of privilege, the information shall be produced in the form of a redacted TIFF image or a party may redact native Excel files by inserting "redacted" where the material is redacted if the producing party maintains a non-redacted version of the Excel.

VII. Production of Audio, Video, and Image Files

A. Audio and video files are to be produced in the native file format in which they were maintained in the ordinary course of business. Produced native audio and video files should be accompanied by a reference file containing the name of the file and hash value for each produced file, if feasible. The audio and video files, as well as all other native files produced, should indicate their native file application in the "File Type" field referenced above, where that metadata field is reasonable available.

B. To the extent audio or video files contain Personally Identifiable Information ("PII"), the files will be produced under the terms of a separate stipulation or order to be agreed upon by the parties or ordered by the Court.

C. Notwithstanding any other provision of this Protocol, image files (e.g., JPEG, HEIC, etc.) that are produced in response to specific requests for production for such image files shall be produced natively with all available EXIF metadata, including location tagging metadata.

VIII. Parent Child Relationships

A. Parent-child relationships (e.g., the associations between emails and their attachments) will be preserved. Email and other ESI attachments will be produced as independent files immediately following the parent email or ESI record. Parent-child relationships will be identified in the data load file as indicated above.

IX. Compressed and Encrypted Files

A. Compressed Files: Compressed file types (i.e., .zip, .rar, .7z) shall be extracted prior to production resulting in the production of individual files.

B. Encrypted Files: The producing party will take reasonable steps, prior to production, to decrypt any password protected files or provide the passwords and any other access requirements for any encrypted files that are produced.

X. Bates Numbering & Document Identifiers

A. Bates numbers and any confidentiality designations shall be electronically branded on each produced TIFF image of ESI.

B. Production Media Unless otherwise agreed, documents and ESI will be produced on optical media (CD/DVD), external hard drive, secure FTP site or similar electronic format. Deliverable media should be encrypted and labeled with the name of the action, the identity of the Producing Party, and the following information: Volume name, production Bates range(s), and the date of delivery

XI. Privilege Log

A. The producing party must also provide a log of any potentially responsive documents withheld on the basis of privilege. Each log entry must contain in separate fields privilege identification number; beginning and ending bates numbers (for redacted documents); author/sender/from; recipients/to; cc; bcc; date of the document; an indication of whether a document is redacted or withheld entirely; the basis for the privilege claim and a description of the privileged content contained within the document and the basis for the privilege assertion sufficiently detailed to enable assessment of the privilege claim.

B. Privileged communications between the client and outside counsel relating to the preparation, prosecution, and/or defense of this lawsuit do not need to be logged; outside counsel's attorney work product related to the same does not need to be logged.

Dated:

SHEPPARD, MULLIN, RICHTER &
HAMPTON LLP

____
Bradley M. Rank
30 Rockefeller Plaza
New York, NY 10112
212-653-8700
brank@sheppardmullin.com

Paul Werner (admitted *pro hac vice*)
Imad Matini (admitted *pro hac vice*)
Hannah Wigger (*pro hac vice* to be
submitted)
2009 Pennsylvania Ave., NW, # 100
Washington, D.C. 20006
202-747-2328
pwerner@sheppardmullin.com
imatini@sheppardmullin.com
hwigger@sheppardmullin.com

Counsel for Defendants

BOIES SCHILLER FLEXNER LLP

*/s/ John T. Zach*____
John T. Zach
David Simons
55 Hudson Yards
New York, NY 10001
212-446-2300
dsimons@bsfllp.com
jzach@bsfllp.com

A. Izaak Earnhardt
1401 New York Ave, NW
Washington, DC 20002
202-237-2727
iearnhardt@bsfllp.com

Counsel for Plaintiff Ryan Berris

SO ORDERED.

____
ARUN SUBRAMANIAN
U.S. District Court Judge
April 17, 2024

APPENDIX 1 – METADATA FIELDS

Field Name	Field Description	Hard Copy	Email	Non-e-mail ESI
BegBates	Beginning Bates number (including Prefix)	x	x	x
EndBates	Ending Bates number (including Prefix)	x	x	x
BegAttach	Beginning Bates number of the first document in an attachment range	x	x	x
EndAttach	Ending Bates number of the last document in attachment range	x	x	x
Custodian/Source	Name of custodian(s) or source of email(s) or file(s) produced	x	x	x
File Type	The record type of document		x	x
Subject	Subject line extracted from an email message		x	
From	From field extracted from an email message		x	
To	To or Recipient extracted from an email or other message		x	
CC	Carbon Copy ("Cc") field extracted from an email message		x	
BCC	Blind Carbon Copy ("Bcc") field extracted from an email message		x	
Sent Date	Sent date and time of e-mail message (Or, if a party has 2 separate fields, date and time can be in separate fields)		x	
Received Date	Received date/time of e-mail message (Or, if a party has 2 separate fields, date and time can be in separate fields)		x	
File Name	Name of file as saved on system			x
Author	The author of the document			x
File Extension	The document extension extracted from document properties			x
Redactions	Yes/No determination advising if the document contains redactions	x	x	x

Confidentiality	Yes/No field or whatever type of Confidentiality is being claimed	x	x	x
Last Modified Date	The application recorded date and time on which the document was last modified (Or, if a party has 2 separate fields, date and time can be in separate fields)			x
Created Date	The application recorded date and time on which the document was created (Or, if a party has 2 separate fields, date and time can be in separate fields)			x
Hash Value	MD5 or SHA-1 hash value used to dedupe the data		x	x
Page Count	Number of pages in the produced document	x	x	x
Native Link (if natives are exchanged)	Relative path to any files produced in native format, such as Excel spreadsheets			x
Text Path	Relative path to any OCR/extracted text files in the production set	x	x	x
Duplicate Custodian	When globally deduping, this field will list for the Producing Party the other custodians that possessed a copy of the document.		x	x